LISTING OF THE CLAIMS

This listing of claims will replace all prior versions, and listings, of claims in the application:

Claims 1-8. (Canceled)

Claim 9. (Original) A method of updating a token, comprising:

accessing a database by user identification and token identification, wherein the database has a plurality of certificates/private keys associated with each token identification;

determining which certificates/private keys of the plurality of certificates/private keys have not been downloaded to the token since the last update;

encrypting all certificates/private keys of the plurality of certificates/private keys which have been not been downloaded to the token using a public key associated with the token identification in the database to form a download packet;

downloading the download packet to the token; and

activating the certificates/private keys in the download packet using the private key in the token.

Claim 10. (Original) A method as recited in claim 9, further comprising:

accessing the database by token identification to identify certificates/private keys which are expired or no longer valid; and

deleting the certificates/private keys identified which are expired or no longer valid form the token.

Claim 11. (Original) The method recited in claim 10, further comprising:

transmitting a message to the user indicating no new certificates/private keys were found in the database when determined that all certificates/private keys of the plurality of certificates/private keys have been downloaded to the token since the last update from the database.

Claim 12. (Currently Amended) The method recited in claim 11, wherein the plurality of certificates/private keys are at least one signature certificate/private key, encryption certificate/private key, and role certificate/private key.

Claim 13. (Original) The method recited in claim 12, wherein the token is a smart card.

Claims 14-17. (Canceled)

Claim 18. (Original) A computer program for updating a token embodied on a computer readable medium and executable by a computer, comprising:

accessing a database by user identification and token identification, wherein the database has a plurality of certificates/private keys associated with each token identification;

determining which certificates/private keys of the plurality of certificates/private keys have not been downloaded to the token since the last update;

encrypting all certificates/private keys of the plurality of certificates/private keys which have been not been downloaded to the token using a public key associated with the token identification in the database to form a download packet;

downloading the download packet to the token; and

activating the certificates/private keys using the private key in the token.

Claim 19. (Original) The computer program as recited in claim 18, further comprising:

accessing the database by token identification to identify certificates/private keys which are expired or no longer valid; and

deleting the certificates/private keys identified which are expired or no longer valid from the token.

Claim 20. (Original) The computer program recited in claim 19, further comprising:

transmitting a message to the user indicating no new certificates/private keys were found in the database when determined that all certificates/private keys of the plurality of certificates/private keys have been downloaded to the token since the last update from the database.

Claim 21. (Currently Amended) The computer program recited in claim 20, wherein the plurality of certificates/private keys are at least one signature certificate/private key, encryption certificate/private key, and role certificate/private key.

Claim 22. (Original) The computer program recited in claim 21, wherein the token is a smart card.

Claim 23. (New) The method recited in claim 9, wherein the activating the certificates/private keys further comprises the entry of a passphrase.

Claim 24. (New) The method recited in claim 9, further comprising:

revoking each certificate/private key associated with a selected token identification for a given token.

Claim 25. (New) The method recited in claim 9, wherein the token identification is assigned by the token manufacturer at the time the token is created and stored in the database when assigned to a user.

Claim 26 (New) The computer program recited in claim 18, wherein the activating occurs in response to receipt of a passphrase.

Claim 27. (New) The computer program recited in claim 18, wherein the token identification is assigned by the token manufacturer at the time the token is created and stored in the database when assigned to a user.

Claim 28. (New) The computer program recited in claim 18, further comprising:

revoking each certificate/private key associated with a selected token identification for a given token.